**TZ-CERT HONEYPOTS WEEKLY REPORT**
**Period : ** 27th August to 2nd of September, 2023
**Report No.:** TZ-CERT/WRHP/2023/35

## 1. NETWORK ATTACKS

A total of **39,100** attacks have been recorded compared to last week **53,365** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords is as in **table1** below:

| SN | ATTACKING IPS | USERNAMES | PASSWORDS |
|---|---|---|---|
| 1. | 218.92.0.92 | root | admin |
| 2. | 185.246.128.133 | admin | 123456 |
| 3. | 193.105.134.95 | postgres | password |
| 4. | 41.78.75.186 | user | 1234 |
| 5. | 41.78.174.124 | ubnt | Win1doW$ |
| 6. | 41.78.73.146 | guest | Admin1234 |
| 7. | 93.179.90.178 | support | cameras |
| 8. | 185.224.128.141 | supervisor | support |
| 9. | 154.92.23.187 | centos | alpine |
| 10. | 148.113.16.121 | dbadmin | (empty) |

*Table1: Top 10 Network attacking IP*

Most of the usernames and passwords listed are commonly used, thus its advised review of usernames and password be made to avoid use of the above listed credentials and default ones. Use of password policies is the best practice.

## 2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **5,029** malicious software distributed compared to last week in which was **21,923.**

Below listed are top ten malicious software and their hashes.

| SN | ATTACKING IPS | MALICIOUS SOFTWARE | HASHES(SHA256) |
|---|---|---|---|
| 1. | 148.113.16.121 | trojan.mirai/xxjvd | 020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0 |
| 2. | 124.29.238.198 | trojan.hajime/siggen | 5c583875c7108394b5437b8ed43501e9d483d5283a5d322425ecbb9c4a97ca71 |
| 3. | 61.223.117.14 | trojan.hajime/genericrxhy | a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3 |

| | | | |
|---|---|---|---|
| 4. | 101.36.108.118 | trojan.hajime/genericrxhy | a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3 |
| 5. | 45.95.146.25 | trojan.hajime/genericrxhy | a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3 |
| 6. | 111.160.116.170 | trojan.xorddos/ddos | ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73 |
| 7. | 188.75.126.74 | trojan.xorddos/ddos | 320b50faf5bcabf75f9547829ee288e09f654db2e8af4d1f2be555ae23a6e85b |
| 8. | 106.75.60.240 | trojan.linux/malxmr | c88e1dacce96cafa2038f7433fc9e42e7b26714c36e98ed59c483360a4b7cb58 |
| 9. | 212.192.11.95 | Riskware/CoinMiner | f2ee717e515f2033bd511ad741f76f2d829bcaad0aeb7b9d0f9091acf43f2297 |
| 10. | 41.78.64.252 | trojan.linux | eaf9adb4bb80316a3aafceabc0f2ed2aed7c76cf134b9b7c66226fc4f003aa97 |

*Table2: Top 10 Malicious attacking IP*

## 3. WEB ATTACKS

During the week the sensors recorded a total of **1,371** web attacks compared to last week which was **1,066.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 27th August to 2nd September, 2023, are detailed. The requests are the payloads.

| SN | ATTACKING IPS | TOP URI |
|---|---|---|
| 1. | 122.155.108.140 | / |
| 2. | 47.115.186.87 | /users/sign_in |
| 3. | 218.161.38.152 | /favicon.ico |
| 4. | 78.31.92.37 | /boaform/admin/formLogin |
| 5. | 78.193.68.134 | /.env |
| 6. | 148.113.16.121 | /administrator/admin/index.php?lang=en |

| | | |
|---|---|---|
| 7. | 41.78.174.124 | /administrator/phpMyAdmin/index.php?lang=en |
| 8. | 41.78.169.54 | /robots.txt |
| 9. | 41.78.75.186 | /__phpmyadmin/index.php?lang=en |
| 10. | 109.237.96.251 | /_phpmyadmin/index.php?lang=en |

*Table3: Top 10 web attacking IP*

## 4. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with most common malware used in the world today. Monitoring of the listed IP address is advised and further to: -

**4.1** Note that most of malicious IP addresses captured are also listed as malicious IP addresses in other sources that are also observing security attacks; thus, security measures should be considered to counter act, including monitoring of the IPs in networks. Most likely the same resources might be used for further attacks.

**4.2** Discourage usage of listed login resources (usernames and passwords) and consider deploying mechanisms to monitor login attempts.

**4.3** Thoroughly check for suspicious files of hashes listed in **Table 2**.

**4.4** Deploy Intrusion Detection System (IDS) and configure to flag detection of attacks associated with list of resources provided especially the IP addresses and the web requests.